Computer Hacker Information Still Available on the Internet!

Vernon Stagg and Matthew Warren
School of Computing & Mathematics
Deakin University
Geelong, Victoria, Australia, 3216

vstagg@deakin.edu.au

Abstract

Knowledge is considered as power. The Internet has become a repository for knowledge. What happens when that information is considered harmful (e.g. how to make bombs, how to hack, etc.)? Society would wish that this information is not made available via the Internet, but the spread of information cannot be stopped. This paper will look at the spread of harmful information and the limitations in trying to control the spread of this information.

Introduction

From humble beginnings as the ARPANET in 1969 through to the pervasive and omnipresent nature of the Internet today, information has been the ultimate objective of this medium. Originally used by scholars to share information and research, the Internet these days provides services and products limited only by the imagination of developers.

Information is available on all kinds of topics - from the beginning of the world to the latest results of your favourite sports. Numerous How-To's and Frequently Asked Questions (FAQ's) exist for novices while more advanced details can be obtained by those with computer savvy. No longer do you need to rummage through old newspaper clippings or visit numerous libraries for that elusive reference, these days nearly everything you need is online.

However, this freedom of information is not without its problems. Personal details, sensitive information, offensive, and illegal material have all appeared in various guises on the Internet. The fundamental nature of the Internet has enabled information to travel freely around the world and to be available from many places at any time. One source of information that has been around since the early days of the Internet is that of hacking.

Hackers

Hackers of the early days were people who would experiment to find machines weaknesses or tweak machines to perform beyond their intended purposes. Through the use of email and bulletin boards, these hackers would post their methods and results, with a hacker culture developing through this interaction. It was not long however before other types of hackers appeared, ones who used their skills to gain unauthorized access to systems, data and software. Many of these hackers also used their skills to override the public telephone system and were known as phreakers. The Internet provided the perfect medium for these people to boast of their "exploits" and provide details on how to reproduce these hacks.

Presented at the 1st Australian Information Security Management Workshop

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Unknown	

4. TITLE AND SUBTITLE
Computer Hacker Information Still Available on the Internet!

5. FUNDING NUMBERS

6. AUTHOR(S)
Vernon Stagg, Matthew Warren

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

School of Computing & Mathematics Deakin University
Geelong, Victoria, Australia, 3216

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Knowledge is considered as power. The Internet has become a repository for knowledge. What happens when that information is considered harmful (e.g. how to make bombs, how to hack, etc.)? Society would wish that this information is not made available via the Internet, but the spread of information cannot be stopped. This paper will look at the spread of harmful information and the limitations in trying to control the spread of this information.

14. SUBJECT TERMS
IATAC Collection, computer hacking, Internet

15. NUMBER OF PAGES
11

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Since many of these hacks went unnoticed, caused little or no damage, or were seen as harmless incidents the general perception of the public towards hacking was relatively indifferent. A number of famous hacks had been documented, such as the break in at LBL computers [STOL89], the Internet worm [SPAF89], and the feats of Kevin Mitnick [HAFF91], but these had minor impact as they did not affect the public at large or have major disruptions to everyday life.

It has only been the last few years that the Internet has become a major component of governments, industries and commercial sectors. The rapid development and deployment of online capabilities and the evolution and implementation of information technologies is transforming society [KAD98]. As Table 1 shows, the growth of the Internet has been staggering with currently over 359 million users worldwide [NUA00].

Date	Number	% Pop
July 2000	359.8 million	5.93
January 2000	248.66 million	4.10
July 1999	185.2 million	4.41
February 1999	153.5 million	3.75
July 1998	129.5 million	3.17
December 1997	101 million	2.47
September 1997	74 million	1.81
December 1996	55 million	1.34
January 1996	30 million	0.73
December 1995	16 million	0.39

Table 1. Number of online users.

In the space of five years, the number of users online has grown by a factor of 22, and this only represents five percent of the world's population! In July of this year, the NEC Research Institute catalogued over 1 billion unique Web pages on the Internet [NEC00]. Table 2 shows a partial breakdown of the survey, indicating the number of individual and mirrored servers discovered.

Number of servers discovered	6,409,521
Number of mirrors in servers discovered	1,457,946
Number of sites (total servers minus mirrors)	4,951,247
Number of good sites (reachable over 10 day period)	4,217,324
Number of bad sites (unreachable)	733,923

Table 2. Internet statistics.

Awareness

In June 1996, the General Accounting Office of the United States released a document entitled "*Information Security: Computer Hacker Information Available on the Internet*" [GAO96A]. A parliamentary testimony, it identified the increasing risks computer hackers pose to computer systems and the proliferation of hacking information available on the Internet. It detailed the access hackers have to numerous tools and techniques that would enable various attacks, active or passive, on computer systems. The tools identified included software that enabled passwords to be broken, data packets to be captured, and vulnerabilities of systems identified. Techniques included methods for bypassing system security measures, rewiring electronic devices, and obtaining system root privileges.

This testimony, along with another report identifying the risks of computer attacks [GAO96B], highlighted the computer and communications security concerns within government, military, and private sectors. These documents indicated the government's awareness of the vulnerability of the Internet and computer systems, the threats that existed, and marked an important change in attitude towards these technologies.

Incidents

The number of computer security incidents has grown rapidly over the years. CERT, the Computer Emergency Response Team, maintains a database of such attacks and has seen a significant number of incident reports since its inception in 1988 [CERT]. Of course, these are only the ones detected or actually reported; the real number would be much higher.

Year	1988	1990	1992	1994	1996	1998	2000 (1st half)
Incidents	6	252	773	2340	2573	3734	8836

Table 3. CERT Number of incidents reported.

The figures obtained by CERT rely on organizations supplying the appropriate details and do not always reflect the real number of actual incidents. Many organizations are loathe acknowledging their weaknesses or may not even be aware of attacks occurring. Others may have political, legal, financial, or security reasons for not disclosing details. Efforts are underway to improve this situation with the development of Information Sharing and Analysis Centers [PDD98] that are intended to remove many of the obstacles in sharing information. The Computer Security Institute recently released its *Computer Crime and Security Survey for 2000* [CSI00], which showed an increase in security incidents with the Internet as a frequent point of attack.

Year	**Incident**			**Point of Attack**		
	Yes	*No*	*Don't know*	*Internal*	*Remote*	*Internet*
1996	42	37	21	53	39	37
1997	50	33	119	52	35	47
1998	64	18	18	44	24	54
1999	62	17	21	51	28	57
2000	70	16	12	38	22	59

Table 4. CSI survey, figures represent percentage of respondents.

Computer attacks can disrupt communications, steal sensitive information, and threaten the ability to execute operations [GAO96a]. Threats are increasing because the number of individuals with computer skills is increasing and because hacking techniques have become readily accessible through magazines and the Internet [GAO00a].

There are significant challenges in controlling unauthorized access and preventing unknown individuals or groups launching untraceable attacks from anywhere in the world [GAO96b]. With technology rapidly developing and costs diminishing, attackers have sophisticated hardware and software to carry out potentially damaging attacks on systems worldwide. Information warfare techniques have become a predominant focus of governments and militaries as they adjust to a new wave of technological defence. The concept of the Toffler's Third Wave [TOFF98] has become a reality as society shifts to an information based economy and information, a sought-after commodity, is no longer regulated or controlled by the traditional dominant power structures such as government or military [KAD98].

Recent computer security incidents have highlighted the debilitating and costly effects that they can have on organizations. The infamous **Melissa** and **ILOVEYOU** viruses had repercussions worldwide, even gaining the spotlight of the world's press, whilst distributed Denial-of-Service attacks on popular sites such as Amazon, Yahoo, and eBay caused significant income losses for these companies[1]. Stories abound of hackers gaining access to confidential information such as credit card details, personal information, medical or financial details, even classified government material.

An information security survey conducted by ICSA identified various concerns held by organizations, including the threat of attack by outsiders. Although insiders are the prime cause of incidents and usually represent the greater risk, outsiders represent an important concern as they:

- Are harder to prosecute
- Often get high profile headline attention
- Can affect shareholder or consumer confidence
- Incidents cannot necessarily be controlled "in-house"
- Attacks may not have a clear purpose
- Attackers may be more organized or focused than an insider

Breach Type	**% Of respondents**				
	Breach detected	*Corruption of information*	*Theft of information*	*Temporary loss of Web site*	*No impact*
Viruses, Trojans, Worms	80	59	7	17	17
Denial of service	37	14	9	40	20
Scripts, mobile code (ActiveX, Java, VBS)	37	44	11	18	28
Protocol weaknesses	26	21	18	23	35
Insecure passwords	25	25	31	14	25
Buffer overflows	24	18	11	34	32
Web server bugs	24	28	13	43	32

Table 5. ICSA survey of detected outside breaches.

[1] Yahoo was flooded with more than 1 gigabit of data per second at the height of the attack. Estimates placed the overall cost of the attacks at US$1 billion [M&W00]

Availability

With the vast number of online users these days, and the enormous amount of information available, it is only inevitable that much of this information will be of a malicious, pernicious, or iniquitous nature. Apart from illegal or inflammatory considerations, much of this information has every right to be available and it is not the intention of this paper to delve into moral, religious, or censorial issues.

Hacker information is readily available on the Internet as well as through other mediums including magazines, CD's, and even television shows. Much of the information is very basic in nature, often outdated, or applicable only to obsolete technology. With a little effort however, information can be found on methods and techniques for hacking that is very applicable for today's technologies.

As part of the GAO report, the phrases "*hacking*" and "*password cracking*" were searched using a popular search engine of the time, Alta Vista[2], with reasonable results [GAO96a]. As a comparison, a search was conducted recently on these phrases, as well as the phrases "*cracking*" and "*hacker tools*", using the same search engine as well as on Google[3]. As the tables below show, there has been a significant increase in hacker information availability!

Search Engine	**Phrase**	
	hacking	*password cracking*
Alta Vista	20,000+	20,000+

Table 6. 1996 Search results

Search Engine	**Phrase**			
	hacking	*password cracking*	*cracking*	*hacker tools*
Alta Vista	297,845	5,414	136,685	2,637
Google	656,000	14,300	421,000	3,910

Table 7. 2000 Search results

Sources

Search engines provide links to numerous hacking information sites. Often these sites contain the same information (mirror sites), have a short life span, or contain links to yet further sites. As well as providing information in the form of documents, many of these sites also offer software, serial numbers, chat lines, newsletters, magazines, or even a bulletin board. Many of these require passwords or advanced knowledge of their existence and often contain more advanced material than generally available.

Other Internet sources for hacking information exist in the form of email, news groups, and archives, including groups such as:

[2] Alta Vista is a search engine that has been available online since 1995, http://www.altavista.com

[3] Google, established in 1998, has become one of the most popular search engines available, with over 1 billion pages indexed, http://www.google.com

- alt.2600;
- alt.hack;
- alt.crack;
- alt.phreaking;
- alt.computer.security;
- comp.security;
- bugtraq;
- cert.

Many of these sites are nothing more than open forums for beginners or "script kiddies" bragging of their exploits or searching for new hacks or cracks. However, occasionally there are important items of information posted that may expose a new vulnerability or code that exploits an unknown weakness.

Some of these and other sites however are more useful to the more advanced or knowledgeable hacker, and can provide valuable information on techniques, newfound weaknesses, or vulnerabilities of computer systems or software.

Hacker Information and Tools: A Simple Scenario

One of the issues in regards to the Internet is that information never disappears, e.g. what happens to a new hacking tool that has been published on the Internet. The tool will be downloaded and mirrored in hacker sites around the world and also added to private software collections. This means that if the initial Web site that offered the tool is closed down, it will appear in a number of other locations around the world. If those sites are closed, the information will just appear on other sites. The proliferatation of destructive information is one of the key factors in helping to promote a culture of Cyber Vandalism [FURN97].

As an example consider a denial of service attack and how a newbie[4] can access the Internet and obtain the required information in order to carry out an attack. A denial-of-service attack results when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user. These attacks do not necessarily damage data directly, or permanently (although possible), but they intentionally compromise the availability of resources and affect the availability of computer systems for legitimate usage. Attacks come in various forms and can include e-mail bomb attacks that systematically send thousands of emails to a particular computer system's email server until that server crashes [WARR00]. A newbie would not need to know this; they can just use user-friendly hacking or denial-of-service tools.

Someone with a minimal level of computer literacy could easily determine that denial-of-service attacks can be a useful means to disrupt organizations. How would they carry an attack without a technical background or knowledge?

Step 1 – Research the topic

They would use the Internet as a research tool, and try to find out about denial-of-service attacks. They would want to determine the different types of attacks, issues behind their usage, and effectiveness of the different technologies. Figure 1 illustrates the results of a quick Internet search, a Web page detailing all the types of denial-of-service attacks and software programs used to launch the attack. The newbie searching for denial-of-service information now realizes that there are software tools that can be used to carry out denial-of-service attacks and selects various tools to use.

[4] A newbie is computer jargon for someone with little or no computing experience.

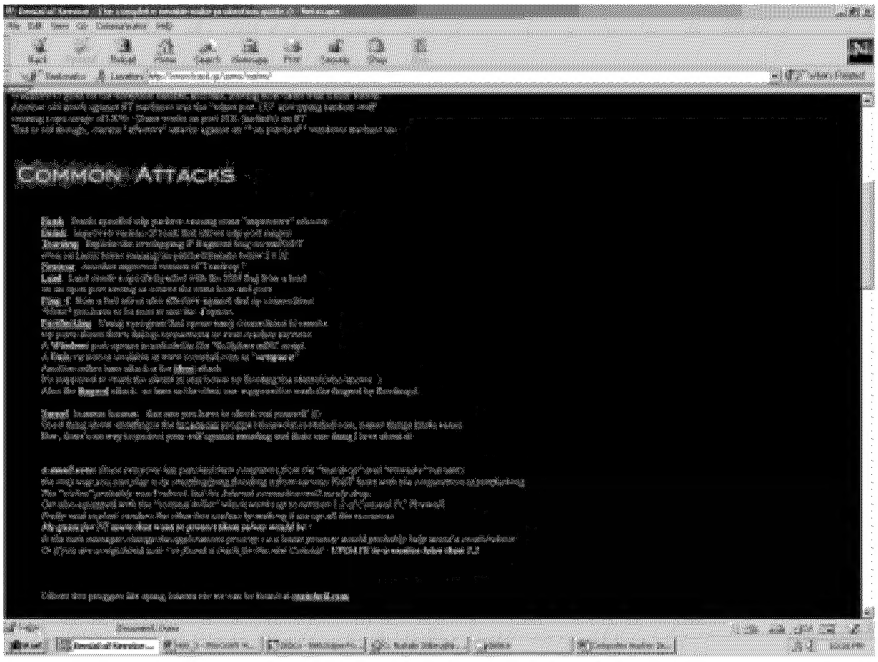

Figure 1: Research into Denial-of-Service

Step 2 – Find the Software

The newbie now knows the names of actual denial-of-service software tools. Another search of the Internet, using the denial-of-service software names as the search query, quickly takes the newbie to hacker software libraries, as illustrated by Figure 2. The newbie can now start to download the software that they require.

Figure 2: Hacker Software Library

Step 3 - Carry out an Attack

The newbie installs the software onto their computer and they are now ready to carry out a variety of denial-of-service attacks. The denial-of-service software prompts them for the required information and then carries out the attack on their behalf; if the user is confused the supporting help files will be able to assist them. Figure 3 shows the results of ten minutes spent on the Internet. The example here shows the newbie with Smurf attack software, Ping of Death attack software, e-mail bomb attack software, IP scanning software and port scanning software. Imagine the damage this individual could inflict upon a small E-commerce organization.

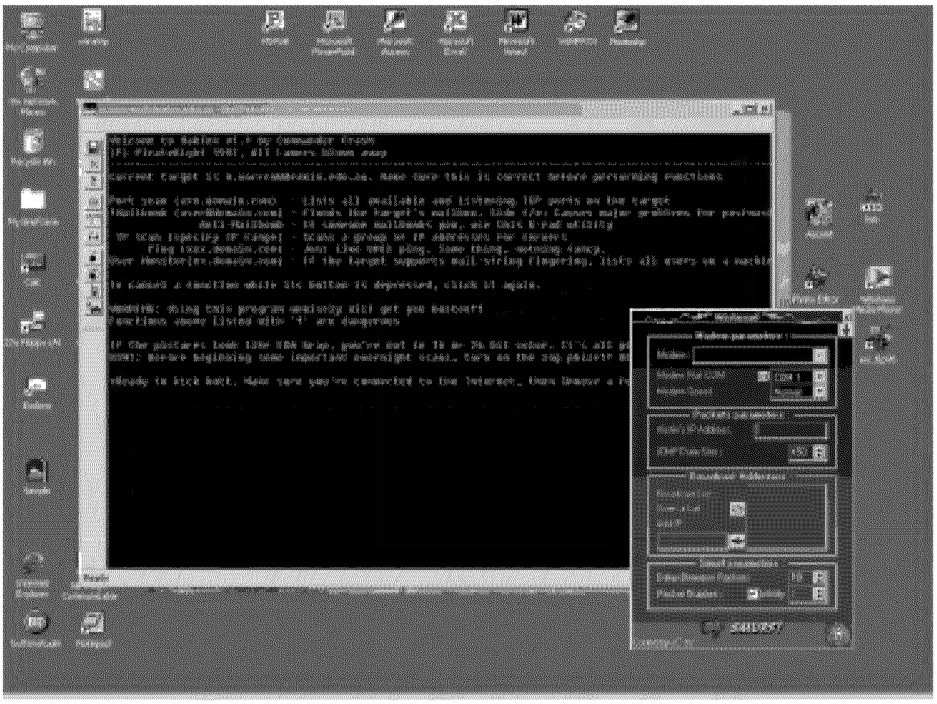

Figure 3: Attack Software ready to be used

This simple scenario illustrates how a person with very limited computer knowledge can find background information and then software to carry out a denial-of-service attack or assist in a hacking attempt. The scenario described took only 15 minutes in real life from Step 1 to Step 3.

Initiatives

Fears of hackers crippling a nation's computer-based services and networks have led to a number of initiatives being developed [MUN96]. The President's Commission on Critical Infrastructure Protection [PCCIP] is one such initiative and represents a concerted effort between government and civilians to protecting their nation's computer-based and computer-controlled infrastructure. Other developments include the European Data Directive [EURO95], the Australian Internet content legislation [BSA99], and the English Investigatory Regulation Bill [RIP00].

Many of these efforts have focused on the threats posed and tend to be prohibitive or disabling in nature, often raising concerns over public and privacy issues. Policies and solutions developed don't necessarily focus on the solution, rather on the vulnerability created [KAD98]. Computer security has a disabling and preventative effect and often adds to the problem rather than solving it.

Hacking is a definite computer security problem and legal, ethical, and moral issues are raised constantly within hacker debates. The traditional defence that a hacker may not set out intentionally to damage a system is a convenient over-simplification of the issue [FURN99]. As Winn Schwartau notes, *the rules seem to be different with computer crime than with physical crime* [SCHW00]. Add to this various international, federal, and state laws, the difficulties involved in tracing cross-border hacker attacks, and the associated costs and the problem suddenly becomes very large.

Acceptance

Hacker information is available on the Internet. This has been seen and will be the case as long as there is an Internet. Efforts and initiatives to control or block information will only have limited success and will cause the information to move underground. The Internet can be utilized as a tool of terror, but it can also be used to facilitate the implementation of solutions to mitigate various threats [KAD98].

Organizations may periodically test their systems and networks using the latest hacking techniques, all which are available on the Internet. Indeed, many testers are encouraged to research and utilise such hacking instructions and tools [GAO98]. While there is much information on hacker tools, they are constantly changing and the side of innovation is always with the hacker [M&W00]. By accepting the existence of these tools and techniques however, policy makers, system administrators and security personnel can utilize them to their own benefit and ensure their systems are reasonably secure[5].

It is essential that those involved with computer security keep abreast of developing techniques, tools, and information about system vulnerabilities [GAO98]. Through timely and accurate information coordination efforts, various entities can provide substantial benefits to system and network defences [KAD98].

There is a certain onus on the entities involved in security to maintain accurate and up-to-date databases on the various techniques and tools available. The dissemination of this knowledge garnered needs to be dispersed in a timely fashion, and, when required, acted upon as determined by its importance. It is no good knowing about vulnerabilities if you do not utilize measures to remove them.

One such instance was the knowledge obtained about distributed denial-of-service attacks. The information was available for organizations to detect the daemon on their system if they had been more attentive [M&W00]. Similarly, the National Infrastructure Protection Center [NIPC] had information available on the ILOVEYOU virus, but did not issue an alert about it till many hours later, too late for many agencies to react [GAO00b].

Conclusion

Modern society is significantly dependent upon Information Technology and communications networks and evidence suggests that this is hardly likely to change in the years ahead. In view of this, it is vital that we are aware of threats such as those highlighted by this paper and take appropriate steps to protect information systems by educating the system administrators, security personnel and users.

[5] Whilst no system can ever be 100% secure, incorporation of hacker techniques and tools into security implementations can enable a more diverse and effective security solution.

We are now in a situation that knowledge can be used repeatedly -- it will not disappear. In fact, it only increases! Digital knowledge can be copied and never missed; it can be given away but still kept. Digital knowledge can be distributed instantly; it is non-linear [FAST00]. In the future we may need to focus on solutions rather than the threats, because the threat will always be there.

References

[BSA99] The Parliament of the Commonwealth of Australia, Broadcast Services Amendment (Online Services) Bill, 1999. http://www.aph.gov.au/parlinfo/billsnet/99077.pdf

[CERT] Computer Emergency Response Team, http://www.cert.org

[CSI00] *2000 CSI/FBI Computer Crime and Security Survey*, Computer Security Issues and Trends, 6:1, Spring 2000. http://www.csi.com

[EURO95] Directive 95/46/EC of the European Parliament, October 1995. http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

[FAST00] Fast, W.R. *Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age*, Institute for National Strategic Studies, 1996. http://www.ndu.edu.inss/siws/ch1.html

[FURN97] Furnell, S.M and Warren, M.J. *Computer Abuse: Vandalising the Information Society,* Internet Research, 7:1, 1997, p 61-66.

[FURN99] Furnell, S.M., Dowland, P.S. and Sanders, P.W. *Dissecting the "Hacker Manifesto"*, Information Management & Computer Security, 7:2, 1999, p 69-75.

[GAO96a] *Information Security: Computer Hacker Information Available on the Internet*, Testimony, United States General Accounting Office, AIMD-96-108, June 1996.

[GAO96b] *Computer Attacks at Department of Defense Pose Increasing Risks*, Report, United States General Accounting Office, AIMD-96-84, May 1996.

[GAO98] *Information Security Management: Learning From Leading Organizations*, Executive Guide, United States General Accounting Office, AIMD-98-68, May 1996.

[GAO00a] *Actions Needed to Address Widespread Weaknesses*, Testimony, United States General Accounting Office, AIMD-00-135, March 2000.

[GAO00b] *Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000*, Testimony, United States General Accounting Office, AIMD-00-229, June 2000.

[HAFF91] Haffner, K. and Markoff, J. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, NY, 1991, pp 368.

[KAD98] Kadner, S., Turpen, E. and Rees, B. *The Internet Information Infrastructure: Terrorist Tool or Architecture for Information Defense?*, Eighth Annual International Arms Control Conference, April 1998.

[M&W00] McCombie, S. and Warren, M. *A Profile of an Information Warfare Attack*, Deakin University, Technical Report TRC-00/08, June 2000, pp 12.

[MUN96] Munro, N. *Sketching a National Information Warfare Defense Plan*, Communications of the ACM, 39:11, November 1996, p 15-18.

[NEC00] *Web Surpasses One Billion Documents*, Inktomi and NEC Research Institute Survey, January 2000. http://www.inktomi.com/webmap/

[NIPC] The National Infrastructure Protection Center, http://www.nipc.gov

[NUA00] *How Many Online*, Worldwide Statistics, NUA Internet Surveys, July 2000, http://www.nua.ie/surveys/how_many_online/world.html

[PCCIP] President's Commission on Critical Infrastructure Protection, Presidential Executive Order 13010, July 1996. http://www.ciao.gov/PCCIP/PCCIP_index.htm

[PDD98] *The Clinton Administration's policy on Critical Infrastructure Protection*, White Paper, Presidential Directive 63, May 1998. http://www.ciao.gov/CIAO_Document_Library/paper598.html

[RIP00] House of Commons, Regulation of Investigatory Powers Bill, February 2000. http://www.homeoffice.gov.uk/ripa/ripact.htm

[SCHW00] Schwartau, W. *Cybershock*, Thunder's Mouth Press, NY, 2000, pp 470.

[SPAF89] Spafford, E.H. *The Internet Worm: Crisis and Aftermath*, Communications of the ACM, 32:6, June 1989, p 678-687.

[STOL89] Stoll, C. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Doubleday, NY, 1989, pp 326.

[TOFF98] Toffler, A. and Toffler, H. *Preparing for Conflict in the Information Age*, The Futurist, June 1998, p 26-29.

[WARR00] Warren, M.J and Hutchinson, W. *Cyber Attacks Against Supply Chain Management Systems*, International Journal of Physical Distribution and Logistics Management, 30:7-8, 2000, p 61-66.